IN THE CLAIMS:

Please amend the claims as follows:

1. (currently amended) A method of enhancing data security comprising:

reading strongly encrypted data external to a secure execution environment of an electronic device to which access is restricted, wherein said strongly encrypted data comprises program code to be executed in said electronic device,

~~generating in a secure execution environment of an electronic device to which access is restricted, a new secret key repeatedly;~~

verifying, in said secure execution environment, the integrity of said strongly encrypted data ~~to be written into storage, wherein said data is to be executed in the electronic device~~;

generating in said secure execution environment of said electronic device to which access is restricted, a new secret key for less strongly encrypting said verified data;

less strongly encrypting, in said secure execution environment, the verified data by means of said new secret key; ~~and~~

writing the less strongly encrypted data into storage, wherein at least some of said storage is external to said secure execution environment, and

repeating each of said above-recited actions.

2. (currently amended) The method according to claim 1, wherein a new secret key is initially generated when the device is booted.

3. (original) The method according to claim 1, wherein a new secret key is generated repeatedly during runtime.

4. (canceled)

5. (previously presented) The method according to claim 1, wherein said storage comprises temporary memory.

6. (previously presented) The method according to claim 1, further comprising:

reordering address locations of said storage in address space at the time of boot, wherein the order of the address locations in address space is altered.

7. (previously presented) The method according to claim 4, further comprising:

authenticating, in said secure execution environment, the program code to be written into storage to ensure that the program code originates from a trusted program code provider.

8. (previously presented) The method according to claim 1, wherein the encrypting data further comprises:

combining the address of the location in said storage, to which location the encrypted data is to be written, with the new secret key; and

using the combination of the address and the new secret key to encrypt said data, wherein the encrypted data becomes associated with said address.

9. (previously presented) The method according to claim 1, wherein the generating a new secret key comprises generating a plurality of new secret keys, wherein each new secret key is used to encrypt a respective subset of the data.

10. (previously presented) The method according to claim 1, further comprising:

calculating, in said secure execution environment, integrity data for data to be stored in said storage; and

storing the calculated integrity data.

11. (original) The method according to claim 10, wherein said integrity data comprises a message authentication code.

12. (original) The method according to claim 11, wherein said message authentication code is calculated by using the generated new secret key.

13. (original) The method according to claim 12, wherein different message authentication codes are calculated for different parts of the data by means of different new secret keys.

14. (previously presented) The method according to claim 13, further comprising:

verifying, in said secure execution environment, correctness of the message authentication code that is associated with read data; and

stopping device operation if said message authentication code is incorrect.

15. (previously presented) The method according to claim 1, further comprising:

setting a processor arranged in the electronic device in one of at least two different operating modes; and

storing protected data relating to device security in at least one storage area of a storage circuitry; wherein

the processor is given access to said storage area, in which said protected data are located, when a secure processor operating mode is set, and

the processor is denied access to said storage area when a normal processor operating mode is set.

16. (original) The method according to claim 15, wherein the setting of processor modes is performed by protected applications.

17. (currently amended) ~~A system~~An apparatus for enhancing data security comprising:

a processor:

arranged to read strongly encrypted data external to a secure execution environment of an electronic device to which access is restricted, wherein said data comprises program code to be executed in said electronic device;

~~arranged to generate in a secure execution environment of an electronic device to which access is restricted, a new secret key in said secure execution environment repeatedly;~~

arranged to verify, in said secure execution environment, the integrity of said strongly encrypted data ~~to be written into storage, wherein said data is to be executed in the electronic device~~;

arranged to generate in said secure execution environment of said electronic device to which access is restricted, a new secret key for less strongly encrypting said verified data;

arranged to less strongly encrypt, in said secure execution environment, the verified data by means of said new secret key; ~~and~~

arranged to write the less strongly encrypted ~~program code~~data into storage, wherein at least some of said storage is external to said secure execution environment, and

arranged to repeat each of said above-recited actions.

18. (currently amended) The ~~system~~apparatus according to claim 17, wherein the system is arranged such that a new secret key is initially generated when the device is booted.

19. (currently amended) The ~~system~~apparatus according to claim 17, wherein the system is arranged such that a new secret key is generated repeatedly during runtime.

20. (canceled)

21. (currently amended) The ~~system~~apparatus according to claim 17, wherein said storage comprises temporary memory external to said secure execution environment.

22. (currently amended) The ~~system~~apparatus according to claim 17, wherein said processor is arranged to reorder address locations of said storage in address space at the time of boot, wherein the order of the address locations in address space is altered.

23. (currently amended) The ~~system~~ apparatus according to claim 20, wherein said processor is arranged to authenticate, in said secure execution environment, the program code to be written into storage to ensure that the program code originates from a trusted program code provider.

24. (currently amended) The ~~system~~apparatus according to claim 17, wherein said processor arrangement to encrypt data further is arranged to combine the address of the location in said storage, to which location the encrypted data is to be written, with the new secret key, and to use the combination of the address and the new secret key to encrypt said data, wherein the encrypted data becomes associated with said address.

25. (currently amended) The ~~system~~apparatus according to claim 17, wherein said processor is

arranged to calculate, in said secure execution environment, integrity data for data to be stored in said storage; and

memory arranged to store the calculated integrity data.

26. (currently amended) The ~~system~~apparatus according to claim 25, wherein said integrity data comprises a message authentication code.

27. (currently amended) The ~~system~~apparatus according to claim 26, wherein said processor arrangement to calculate is arranged such that it uses the new secret key generated to calculate the message authentication code.

28. (currently amended) The ~~system~~ apparatus according to claim 27, wherein said processor is

arranged to verify, in said secure execution environment, correctness of the message authentication code that is associated with read data and to stop device operation if said message authentication code is incorrect.

29. (currently amended) The ~~system~~apparatus according to claim 17, wherein said processor is

arranged such that it may be set in one of at least two different operating modes; and wherein said system further comprises

storage circuitry arranged with at least one storage area in which protected data relating to device security are located; wherein the system is further arranged such that:

the processor is given access to said storage area, in which said protected data are located, when a secure processor operating mode is set, and

the processor is denied access to said storage area when a normal processor operating mode is set.

30. (currently amended) The ~~system~~apparatus according to claim 29, wherein the setting of processor modes is performed by protected applications.

31. (currently amended) A mobile telecommunication terminal comprising the ~~system~~apparatus according to claim 17.

32. (currently amended) A programmable logic device comprising the ~~system~~ apparatus according to claim 17.

33. (previously presented) The programmable logic device according to claim 32, wherein said programmable logic device is implemented in the form of an application specific integrated circuit.

34. (previously presented) A computer program product comprising computer-executable components stored in a memory for causing a device to perform the actions recited in claim 1 when the computer-executable components are run on a processing unit included in the device.

35. (previously presented) A computer-readable medium storing computer-executable components for causing a device to perform the actions recited in claim 1 when the computer-executable components are run on a processing unit included in the device.

36. (currently amended) ~~A system~~An apparatus for enhancing data security comprising:

means for reading strongly encrypted data external to a secure execution environment of an electronic device to which access is restricted, wherein said data comprises program code to be executed in said electronic device;

~~means for generating, in a secure execution environment of an electronic device to which access is restricted, a new secret key in said secure execution environment repeatedly;~~

means for verifying, in said secure execution environment, the integrity of said strongly encrypted data ~~to be written into storage which data is to be executed in the electronic device~~;

means for generating, in said secure execution environment of said electronic device to which access is restricted, a new secret key for less strongly encrypting said verified data;

means for less strongly encrypting, in said secure execution environment, the data by means of said new secret key; ~~and~~

means for writing the less strongly encrypted ~~program code~~data into storage, wherein at least some of said storage is external to said secure execution environment, and

means for repeating the above-recited functions.